

IN THE CLAIMS

Please amend the claims to read as follows:

Listing of Claims

Claims 1-39 (Cancelled).

40. (New) A data processing system for performing authentications and business transactions comprising:

at least one local client configured to support at least one network connection;

at least one authentication server configured to perform authentications according to a predetermined authentication policy and further configured to support at least one network connection;

an intelligent portable device configured to support a PSD, at least one device connection and at least one network connection; and

a PSD which is functionally connected to said intelligent portable device and configured to generate authentication information according to said predetermined authentication policy, and which is associated to an identified user, wherein:

said at least one local client and said at least one authentication server are functionally connected to each other over at least one network connection,

said predetermined authentication policy is functionally stored within said PSD and said at least one authentication server, and

said at least one local client comprises an activator of an authentication according to said authentication policy between said PSD and said at least one authentication server upon an action of said identified user on said at least one local client.

41. (New) The data processing system according to claim 40, wherein:

said at least one local client is configured to support at least one device connection; and

said intelligent portable device is functionally connected to said at least one local client through said at least one device connection of said at least one local client and further configured as a hardware device peripheral which allows the PSD to communicate said authentication information to said at least one authentication server using said at least one network connection of said at least one local client.

42. (New) The data processing system according to claim 41, wherein said device connection between said at least one local client and said intelligent portable device is selected from the group consisting of a direct connection, an optical connection, a wireless RF connection or an electro-acoustical connection.

43. (New) The data processing system according to claim 40, wherein said predetermined authentication policy includes asynchronous authentication means, synchronous authentication means and cryptography means.

44. (New) The data processing system according to claim 40, comprising at least two local clients respectively functionally connected to at least two authentication servers over at least one network connection, wherein each of said at least two local clients is configured to support at least one device connection, and wherein said intelligent portable device is functionally connected to each of said at least two local clients through said at least one device connection of each of said at least two local clients and further configured as a hardware device peripheral.

45. (New) The data processing system according to claim 40, wherein said intelligent portable device is functionally connected to said at least one authentication server through at least one network connection and configured as an independent portable device which allows the PSD to communicate said authentication information to said at least one authentication server using said at least one network connection.

46. (New) The data processing system according to claim 45, wherein said at least one network connection between said at least one authentication server and said intelligent portable device is selected from the group consisting of a wireless RF network and a digital cellular network.

47. (New) The data processing system according to claim 45, wherein said intelligent portable device is functionally connected to said at least one authentication server through at least two network connections over at least two networks, a first network connection being dedicated for sending a first portion of said authentication information and a second network connection being dedicated for sending a second portion of said authentication information.

48. (New) The data processing system according to claim 40, wherein a plurality of network and device connections are facilitated using said intelligent portable device.

49. (New) The data processing system according to claim 40, wherein said intelligent portable device is configured as a hardware device peripheral.

50. (New) The data processing system according to claim 40, wherein said intelligent portable device is configured as an independent intelligent portable device.

51. (New) The data processing system according to claim 40, wherein said predetermined authentication policy includes asynchronous authentication means and cryptography means.

52. (New) The data processing system according to claim 40, wherein said predetermined authentication policy includes synchronous authentication means and cryptography means.

53. (New) A method for performing authentications and business transactions comprising:

networking an intelligent portable device configured to support a functionally connected PSD, to at least one authentication server using a network connection, wherein a shared predetermined authentication policy is functionally stored in said at least one authentication server and said PSD;

initiating an authentication request by an identified user on at least one local client, wherein said identified user is associated with said PSD;

sending the request to said at least one authentication server, wherein said at least one local client and said at least one authentication server are functionally connected to each other by a network;

authenticating said identified user using said predetermined authentication policy between said PSD and said at least one authentication server; and

allowing said identified user access to the network following successful authentication for purposes of performing additional transactions.

54. (New) The method according to claim 53, wherein said authentication request includes at least one unique identifier associated with said identified user.

55. (New) The method according to claim 54, wherein said at least one unique identifier is used by said at least one authentication server for locating and communicating with said intelligent portable device associated with said identified user.

56. (New) The method according to claim 54, wherein said at least one unique identifier is used by said at least one authentication server for locating and communicating with another intelligent portable device associated with a second level approver.

57. (New) The method according to claim 53, wherein a plurality of authentications are facilitated using said shared predetermined authentication policy.

58. (New) The method according to claim 53, further comprising an authentication of said identified user to said PSD by entry of a Personal Identification Number.

59. (New) The method according to claim 53, further comprising an authentication of said identified user to said PSD by entry of a biometric result.

60. (New) The method according to claim 58 or 59, wherein said entry is conducted using a user interface and display associated with said intelligent portable device.

61. (New) The method according to claim 58 or 59, wherein said entry is conducted using a user interface and display associated with said at least one local client.

62. (New) The method according to claim 58 or 59, wherein exceeding a maximum number of attempts at authentication ends the authentication.

63. (New) The method according to claim 53, wherein said shared predetermined authentication policy includes asynchronous authentication and cryptography, and wherein exceeding a predetermined response time ends the authentication.

64. (New) The method according to claim 53, further comprising business transactions.

65. (New) An intelligent portable data processing device for performing authentications and business transactions comprising a user interface, a display, data processing means,



data storage means, at least one device connection and at least one network connection, further comprising:

a PSD configured to generate authentication information according to a predetermined authentication policy which is shared with at least one remote authentication server, wherein said PSD is associated to an identified user; and

means for transferring to the PSD a request for authentication with said at least one authentication server, using said shared predetermined authentication policy, upon reception of said request, if said request contains an identifier of said identified user.

66. (New) The intelligent portable data processing device according to claim 65, functionally connected to at least one local client using said at least one device connection.

67. (New) The intelligent portable data processing device according to claim 65 or 66, functionally connected to at least one authentication server using said at least one network connection.

68. (New) The intelligent portable data processing device according to claim 65, functionally connected to a plurality of local clients using said at least one device connection.

69. (New) The intelligent portable data processing device according to claim 65 or 68, functionally connected to a plurality of authentication servers using said at least one network connection.

70. (New) The intelligent portable data processing device according to claim 65, wherein the PSD is a physical device.

71. (New) The intelligent portable data processing device according to claim 65, wherein the PSD is a virtual device.